

REMARKS

The Office Action dated November 15, 2005 has been received and its contents carefully noted. By the above actions, claims 1-33 are pending in the application. In order to better define that which Applicants regard as the invention, claims 1 and 15 have been amended. No new matter has been added. Support for the amendments is provided in the original claims, Figures 1-14, and related text of the specification.

In view of these actions and the following remarks, reconsideration of this application is now respectfully requested.

Rejections under 35 U.S.C. §102

Claims 1, 4-7, 12-15, 19-21, 24-25, and 27-33 are rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Pat. No. 6,084,969 to Wright et al. Applicant respectfully traverses this rejection, because Wright et al. fails to teach each and every element recited by the claims. In particular, amended claims 1 and 15 now recite that “the encrypted message remains encrypted during the transformation.” As the present specification states, “The introduction of proxy keys and transformations must in no way compromise security and privacy of the encryption. Thus, it should be at least computationally hard for any unauthorized third party to recover the original message and decryption keys of the grantor and grantee from publicly available information.” (See present specification, p. 22, lines 22-26, emphasis added.) Wright et al., however, teaches “using a pager proxy to carry out decryption of a message encrypted by a session key and received from the sending pager, and to have the pager proxy generate a new session key for re-encryption of the message transmitted to the receiving pager. . .” (See Wright et al., col. 4, line 65-col. 5, line 2, emphasis added.) Contrary to claims 1 and 15, the encrypted message in Wright et al. does not remain encrypted during application of a new key to the message.

It is noted that the Examiner points to column 14, lines 61-67 of Wright et al., which state that “although the preferred embodiment of the invention has the pager proxy re-package the message by first decrypting it, and then re-encrypting it using a new session key, it is also within the scope of the invention to have the pager proxy decrypt only the session key and re-encrypt the same session key using the public key or shared secret key of the destination pager.” As Wright et al. explains, the pager proxy decrypts (and re-encrypts) only the session key. Although the message remains encrypted, it is not transformed by the

application of a public proxy key, as recited by claims 1 and 15. Like the other embodiments taught by Wright et al., this alternative embodiment cited by the Examiner still fails to disclose, or even suggest, a process where the encrypted message remains encrypted while also being transformed by the application of a public proxy key. Moreover, the session key in this alternative embodiment is actually a “message,” which is initially encrypted but is subsequently decrypted before re-encryption with a the new key. Indeed, this alternative embodiment clearly establishes that Wright et al. requires the decryption of an object before any application of a new key to that object. Accordingly, because Wright et al. actually teaches away from applying a public proxy key to transform an encrypted message while keeping the message encrypted during transformation, withdrawal of this rejection of claims 1 and 15 is in order and is respectfully requested.

Furthermore, independent base claim 1 recites “generating a public proxy key based on a private key corresponding to the recipient and on the private key corresponding to said grantor, wherein said grantor’s private key and said recipient’s private key are combined, and the combination of the private keys is based on said public key encryption scheme.” In addition, independent base claim 15 recites “generating a public proxy key based on a public key corresponding to the recipient and on the private key corresponding to the public key of said grantor, wherein said grantor’s private key and said recipient’s public key are combined, and the combination of said grantor’s private key and said recipient’s public key is based on said public key encryption scheme.” Contrary to the Examiner’s assertions, Wright et al. does not disclose, or even suggest, using a public proxy key based on the combination of a key corresponding to the grantor and a key corresponding to the recipient, as recited in claims 1 and 15. The Examiner cites column 5, lines 2-4 of Wright et al. as anticipating this limitation in claim 1. In addition, the Examiner cites column 5, lines 2-5 and column 7, lines 64-67 of Wright et al. as anticipating this limitation in claim 15. However, Column 5, lines 2-5 of Wright et al. teach that “. . . the original session key [is] encrypted at least by a secret key shared by the sending pager and the pager proxy server or by a public key corresponding to a private key of the pager proxy server. . .” Neither the “secret key shared by the sending pager and the pager proxy server” nor the “public key corresponding to a private key of the pager proxy server” of Wright et al. can be considered to be the public proxy key recited in claims 1 and 15. Moreover, Column 7, lines 64-67 of Wright et al. merely states that “[t]he public-private key encryption algorithms are preferred not only because of the strong encryption provided, but also because the [sic] permit authentication of the sender. . .” The

sections from Wright et al., cited by the Examiner, clearly fail disclose anything about generating a public proxy key by combining a key corresponding to the grantor and a key corresponding to the recipient.

Accordingly, because Wright et al. fails to disclose both the steps of generating a public proxy key and applying the public proxy key as recited by independent claims 1 and 15, Wright et al. fails to disclose each and every element recited by the claims. Thus, withdrawal of the rejection of independent claims 1 and 15 is in order and is respectfully requested. In addition, Applicant respectfully submits that dependent claims 4-7, 12-14, 19-21, 24-25, and 27-33 are allowable, since they depend on what is now believed to be allowable base claims 1 and 15.

Rejections under 35 U.S.C. §103

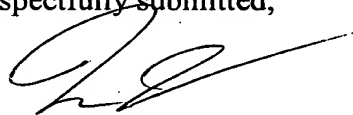
Claims 2-3, 8-11, and 22-23 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Wright et al., in further view of U.S. Pat. No. 5,748,736 to Mittra. Applicant respectfully submits that dependent claims 2-3, 8-11, and 22-23 are allowable, since they depend on what is now believed to be allowable base claims 1 and 15. Applicant also respectfully traverses this rejection, because Mittra fails to disclose the encryption scheme as recited in claims 2, 3, 22, and 23. In particular, dependent claims 2, 3, 22, and 23 recite that the encrypted message has been encrypted with an ElGamal or a modified ElGamal encryption scheme. The Examiner concedes that Wright et al. "fails to include an ElGamal encryption scheme" and relies upon Mittra to cure this deficiency. (See Office Action, p. 9, lines 15-21.) However, Mittra discloses only the use of the "ElGamal signature scheme" and not an ElGamal encryption scheme. (See Mittra, col. 10, line 67.) The ElGamal encryption scheme (a non-deterministic encryption using a public key relying upon digital logarithm) is used for encryption purposes while the ElGamal signature scheme is for source authentication and sender non-reputation purposes. The ElGamal encryption scheme and the ElGamal signature scheme employ different algorithms and computations and are not the same. Therefore, Applicant respectfully submits that the cited references fail to disclose all the elements recited in dependent claims 2, 3, 22, and 23.

Claims 18 and 26 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Wright et al., in further view of Irish Times "Encryption Technology to Thwart Computer Hackers System Should Protect Security of E-Commerce" (City Edition). Applicant

respectfully submits that dependent claims 18 and 26 are allowable, since they depend on what is now believed to be allowable base claims 1 and 15.

In light of the amendments to the claims and the remarks provided hereinabove, the present application is now believed to be in condition for allowance. However, should the Examiner find some issue to remain unresolved, or should any new issues arise, which could be eliminated through discussions with Applicant's representative, then the Examiner is invited to contact the undersigned by telephone in order that further prosecution of this application can thereby be expedited.

Respectfully submitted,



Marc S. Kaufman
Registration No. 35,212

Nixon Peabody LLP
401 9th Street, N.W. Suite 900
Washington, D.C. 20004-2128
(202) 585-8000